BUNDESREPUBLIK DEUTSCHLAND

#4
12-27-00
12-26-01

Bescheinigung

Die Firma International Business Machines Corp. in Armonk, N.Y./V.St.A. und die Siemens Aktiengesellschaft in München/Deutschland haben eine Patentanmeldung unter der Bezeichnung

"Sicheres Personalisieren von Chipkarten"

am 19. August 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 06 F 17/60 der Internationalen Patentklassifikation erhalten.

München, den 15. März 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Aktenzeichen: 199 39 280.3

Nietied

B E S C H R E I B U N G

Sicheres Personalisieren von Chipkarten

Die Erfindung betrifft ein Verfahren zum Initialisieren und Personalisieren einer Chipkarte und eine entsprechende Chipkarte.

Bei der Herstellung von Chipkarten gibt es zwei Produktionsschritte, die sich mit dem Aufbringen von Daten auf die Chipkarte beschäftigen, Initialisierung und Personalisierung.

Während der Initialisierung werden im Speicher der Chipkarte die später benötigten Strukturen, beispielsweise Dateien, Verzeichnisse und deren Zuordnung zueinander, angelegt. Weiterhin werden Daten auf die Chipkarte aufgebracht, die für alle Chipkarten einer Serie gleich sind. Bei der Initialisierung ist die Geschwindigkeit als Kostenfaktor von Bedeutung.

Während der Personalisierung werden geheime und/oder kartenspezifische Informationen auf die Chipkarte aufgebracht. Wurde beispielsweise bei der Initialisierung die Nummer der Kartenorganisation eingetragen, die für alle Chipkarten gleich ist, so wird bei der Personalisierung beispielsweise die Kreditkartennummer, die karten-individuell ist, in den Speicher der Chipkarte programmiert. Eine wichtige Anforderung dabei ist, dass eine Personalisierung nur für diejenigen Datenfelder möglich ist, die für eine Personalisierung vorgesehen sind. Es muß sichergestellt werden, dass die Daten an die richtige Stelle, d.h. nur in die bei der Initialisierung vorgesehenen Personalisierungsdatenfelder geschrieben werden. Diese Anforderung wird bisher dadurch gelöst, daß während der

Initialisierung sogenannte Platzhalter in den Speicher der Chipkarte eingebracht werden. Bei der Übertragung von Personalisierungsdaten in ein Personalisierungsdatenfeld während der Personalisierung werden dann zusätzliche Informationen, zusammen mit den Personalisierungsdaten, an die Chipkarte übergeben. Anschließend werden diese zusätzlichen Informationen mit den Informationen verglichen, die in dem Platzhalter gespeichert sind. Sind diese identisch, werden die Personalisierungsdaten in den Speicher der Chipkarte geschrieben. Diese Prüfung ist jedoch nicht derart robust, daß eine Fehlverwendung auszuschließen wäre. Es sind Chipkarten bekannt, auf die mehrere Chipkarten-anwendungen geladen werden. Eine Chipkartenanwendung ist ein Dienst, der mit der Chipkarte ausgeführt werden kann, beispielsweise eine Zahlungsfunktion (Chipkartenanwendung A) oder ein elektronischer Führerschein (Chipkartenanwendung B). Für die Gewährleistung der Sicherheit bei der Personalisierung der Chipkarte ist es dabei erforderlich, die Chipkartenanwendungen bei der Personalisierung zu trennen, d.h. sicherzustellen, dass ausschließlich der Anbieter der Chipkartenanwendung A in der Lage ist, die Chipkartenanwendung A zu personalisieren, also Daten für die Chipkartenanwendung A auf die Chipkarte aufzubringen. Gleiches gilt für den Anbieter der Chipkartenanwendung B und für jede weitere Chipkartenanwendung. Eine sichere Trennung der Chipkartenanwendungen bei der Personalisierung wurde bisher in keinem Chipkarten-Personalisierungssystem realisiert.

Es ist Aufgabe der vorliegenden Erfindung, ein Verfahren zum verbesserten Initialisieren und Personalisieren von Chipkarten und eine entsprechende Chipkarte bereitzustellen.

Erfindungsgemäß wird diese Aufgabe durch die unabhängigen Ansprüche gelöst.

Entsprechend der vorliegenden Erfindung werden auf der Chipkarte Datenstrukturen angelegt, die eine eindeutige Zuordnung der bei der Personalisierung auf die Chipkarte zu übertragenden Daten zu den einzelnen Chipkartenanwendungen und damit zu den Anbietern dieser Chipkartenanwendungen ermöglicht. Dadurch wird eine sichere Trennung der Chipkartenanwendungen bei der Personalisierung realisiert. Mit der vorliegenden Erfindung wird es, beispielsweise den Anbietern von Chipkartenanwendungen, während der Personalisierung unmöglich gemacht, Personalisierungsdaten in nicht dafür vorgesehene Personalisierungsdatenfelder zu schreiben. Die vorliegende Erfindung erlaubt eine robuste Personalisierung der bei der Initialisierung definierten Personalisierungsdatenfelder, wobei nur die dafür vorgesehenen Speicherzellen des Chipkartenspeichers personalisiert werden können. Bei der Anwendung der vorliegenden Erfindung wird kein zusätzlicher Speicherplatz im Chipkartenspeicher benötigt. Die für eine derartige Personalisierung erforderliche Initialisierung erfolgt dabei ohne Geschwindigkeitseinbußen im Vergleich zu herkömmlichen Initialisierungsverfahren.

Die Erfindung ist nachstehend anhand von bevorzugten Ausführungsformen näher beschrieben. Es zeigt:

Fig.1 den schematischen Aufbau einer Chipkarte mit Datenspeicher und einzelne Speicherblöcken,

Fig.2 den schematischen Aufbau zweier Personalisierungsbeschreibungen (PD) und ihre logische Verbindung nach der vorliegenden Erfindung,

Fig.3 den schematischen Aufbau einer Anwendungsbeschreibung (AD) und zweier Personalisierungsbeschreibungen (PD) und ihre logischen

Verbindungen miteinander nach der vorliegenden Erfindung,

Fig.4 den Datenspeicher einer Chipkarte nach einer erfindungsgemäßen Initialisierung,

Fig.5 den Datenspeicher einer Chipkarte während einer erfindungsgemäßen Personalisierung,

Fig.6 den Ablauf einer Personalisierung entsprechend der vorliegenden Erfindung.

Fig.1 zeigt eine Chipkarte 100, wie sie in einer bevorzugten Ausführungsform der vorliegenden Erfindung verwendet wird. Dabei handelt es sich bei der Chipkarte um eine sogenannte Smartcard, also eine Chipkarte mit Prozessor 101, Datenspeicher 102 und Software, zum Beispiel dem Chipkartenbetriebssystem. Bevorzugt wird dabei der Datenspeicher 102 der Chipkarte 100 mittels einer Speicherverwaltung verwaltet, die sich auf der Chipkarte 100 befindet, und zum Beispiel Teil des Chipkartenbetriebssystems ist. Die Speicherverwaltung unterteilt den Datenspeicher 102 der Chipkarte 100 in einzelne Speicherblöcke 103. Diese Unterteilung erfolgt bevorzugt dynamisch, d.h. je nach Speicherplatzanforderung der einzelnen Betriebssystemfunktionen oder Chipkartenanwendungen. Jeder Speicherblock 103 verfügt über eine physikalische Adresse, die von der Speicherverwaltung verwaltet wird. Da diese Adressen von der aktuellen Chipkartenbetriebssystemversion der verwendeten Chipkartenhardware und anderen Randbedingungen abhängig ist, wird in der bevorzugten Ausführungsform mit Offset-Angaben gearbeitet. Soll nun ein Speicherbereich im Datenspeicher 102 der Chipkarte 100 initialisiert werden, beispielsweise zum Anlegen einer Datei, wird über ein Chipkartenkommando, beispielsweise CREATE FILE, ein freier Speicherblock 103,

zugewiesen und gegebenenfalls mit Daten beschrieben. Für das Schreiben von Daten in einen bestimmten Bereich innerhalb dieses Speicherblockes 103 wird bevorzugt wiederum ein Offset, beispielsweise bezogen auf den Anfang des Speicherblocks 103, verwendet. Durch die Verwendung relativer Speicheradressen wird eine Abstraktion von hardware-spezifischen, physikalischen Speicheradressen erreicht.

Im folgenden wird die Initialisierung beschrieben, die zur Vorbereitung der Personalisierung der Chipkarte 100 dient.

Während der Initialisierung wird an jede Stelle innerhalb eines Speicherblockes 103, die ein Personalisierungsdatenfeld aufnehmen soll, eine Personalisierungsbeschreibung, der sogenannte Personalization Descriptor (PD) geschrieben. Fig.2 zeigt den Aufbau eines PD 200. Dabei enthält jede Personalisierungsbeschreibung ein Offsetfeld NEXT 203. Zusätzlich kann jede Personalisierungsbeschreibung ein Längenfeld LEN 201 und ein Statusfeld FLAG 202 enthalten. Zur Beschreibung von weiteren Personalisierungseigenschaften ist das Einfügen weiterer optionaler Felder möglich.

Ist es für die Personalisierung einer Chipkartenanwendung erforderlich, mehr als einen Personalisierungsdatensatz zu übertragen, werden während der Initialisierung entsprechende Speicherzellen im Datenspeicher 102 der Chipkarte 100 durch weitere PDs reserviert. Das Offsetfeld NEXT 203 des PD 200 gibt den Offset, also die Speicheradresse, eines weiteren PD 210 an. Über das Offsetfeld 203 werden die erforderlichen PDs 200, 210 in PD-Listen organisiert, so daß für die Personalisierung eine Reihe von PDs 200, 210, ... in einer bestimmten Reihenfolge feststehen. Die PDs 200, 210, ... sind dabei in der gleichen Reihenfolge im organisatorischen Sinne miteinander verbunden, in der die Personalisierungsdaten während der anschließenden Personalisierung an die

Chipkarte 100 übergeben werden. Enthält die PD-Liste keine weiteren Elemente, oder besteht die PD-Liste aus lediglich einem Element, so kann das beispielsweise dadurch gekennzeichnet werden, dass das Offsetfeld 203 des letzten PD den Inhalt Null hat. In Fig.2 ist die Verbindung zweier PDs, hier PD1 und PD2, zu einer PD-Liste dargestellt. Durch die Verwendung relativer Speicheradressen wird, wie oben beschrieben, eine Abstrahierung von den physikalischen Adressen erreicht, was insbesondere dann vorteilhaft ist, wenn nachträgliche Änderungen an der Chipkartenhardware oder dem Chipkartenbetriebssystem vorgenommen werden müssen.

Um die Robustheit der Personalisierung zu erhöhen, kann das optionale Längenfeld LEN 201 eingeführt werden. Im Längenfeld LEN 201 des PD 200 wird dabei die Länge, beispielsweise in Bytes, des Personalisierungsdatenfeldes angegeben, welches während der späteren Personalisierung an die Stelle des PD 200 tritt, zu dem das Längenfeld 201 gehört.

Bevorzugt ist die Länge eines während der Initialisierung in den Datenspeicher 102 geschriebenen PD 200 kleiner als die Länge des später übertragenen Personalisierungsdatenfeldes. Beispielsweise beträgt die Länge eines PD 4 Byte, wohingegen die Länge eines Personalisierungsdatenfeldes beispielsweise 40 Byte beträgt. Ein PD 200 kann aber auch ebenso groß wie das dazugehörige Personalisierungsdatenfeld sein. Durch die Einführung des Längenfeldes 201 ist ein Schutz gegen das Zerstören der initialisierten Speicherstrukturen möglich.

Zur Erhöhung der Sicherheit während des Personalisierens kann das optionale Statusfeld FLAGS 202 eingeführt werden. Das Statusfeld 202 eines PD 200 dient zur Speicherung verschiedener Statusbits, sogenannten flags, die festlegen, welche Eigenschaften die Personalisierungsdaten besitzen müssen, die bei der Personalisierung an die Stelle des PD

200 geschrieben werden sollen. Beispielsweise kann somit festgelegt werden, ob die Personalisierungsdaten verschlüsselt/unverschlüsselt und/oder signiert/unsigniert etc. sein müssen.

Mit der Einführung dieser erweiterten Personalisierungsbeschreibungen wird eine für jeden Personalisierungsdatensatz individuell definierbare Steuerung des Personalisierungsverfahrens ermöglicht.

Zusätzlich wird während der Initialisierung für jede Chipkartenanwendung mindestens eine Anwendungsbeschreibung, ein sogenannter Application Descriptor (AD), im Datenspeicher 102 der Chipkarte 100 angelegt. Da die Chipkartenanwendungen jeweils einem Anbieter zugeordnet sind, sind auch die ADs den Anbietern der Chipkartenanwendungen zugeordnet. Den Aufbau eines AD 300 zeigt Fig.3.

Ein AD 300 umfaßt zur Identifizierung des AD eine Anwendungsbezeichnung 301, die diejenige Chipkartenanwendung bezeichnet, deren Personalisierung unter Verwendung des AD 300 durchgeführt werden soll. Die Anwendungsbezeichnung 301 wird im folgenden auch mit Application Identifier (AID) bezeichnet. Vorzugsweise umfaßt der AID 301 dabei den Namen der entsprechenden Chipkartenanwendung sowie eine eindeutige numerische Identifikation des AD 300.

Weiterhin umfaßt der AD 300 den Offset ACT 302 des nächsten zu bearbeitenden PD. Dabei wird das Offsetfeld 302 so initialisiert, daß es vor Beginn der Personalisierung auf den ersten PD 200 einer PD-Liste zeigt.

Zusätzlich kann der AD 300 weitere Daten, beispielsweise Schlüsseldaten KEY 303 für die Anwendung kryptographischer Sicherheitsmechanismen, zum Beispiel für die Entschlüsselung

der verschlüsselt übertragenen Personalisierungsdaten oder für die Überprüfung einer Signatur enthalten. Das erlaubt jedem Anbieter von Chipkartenanwendungen die individuelle Gestaltung der anzuwendenen kryptographischen Sicherungsverfahren während der Personalisierung.

Weiterhin kann der AD 300 auch einen Fehlbedienungszähler CNT 304 umfassen. Zur Erhöhung der Robustheit der Personalisierung kann der AD 300 des weiteren einen sogenannten Sequence Counter SEQ 305 umfassen, einen Zähler, der bei jedem erfolgreichen Eintragen eines Personalisierungsdatensatzes in den Datenspeicher 102 der Chipkarte 100 inkrementiert wird, und beispielsweise während der Personalisierung zur Synchronisation mit externen Datenbankanwendungen eingesetzt werden kann.

Ein PD 200, 210, ... kann jeweils nur einer PD-Liste zugeordnet sein, wobei jede PD-Liste jeweils einem bestimmten AD 300, und damit einer Chipkartenanwendung zugeordnet ist. Sollen sich mehrere Chipkartenanwendungen auf der Chipkarte 100 befinden, müssen demnach auch mehrere PDs oder PD-Listen vorhanden sein. Damit wird eine Trennung der Chipkartenanwendungen erreicht. Durch die beschriebene Art der Initialisierung mit einer Listenorganisation der PDs 200, 210, ... und einer Kopplung der einzelnen PD-Listen an je einen AD 300 ist eine eindeutige Zuordnung der Personalisierungsfelder zu den verschiedenen Anbietern der jeweiligen Chipkartenanwendungen gegeben. Da ein AD 300 jeweils nur einer Chipkartenanwendung zugeordnet ist, werden sicherheitsrelevante Daten, wie Schlüsseldaten KEY 303, eindeutig einer bestimmten Chipkartenanwendung zugeordnet.

Nach den beschriebenen Initialisierungsschritten zur Vorbereitung der Personalisierung ergibt sich beispielhaft das in Fig.4 gezeigte Speicherabbild, in dem auch die logischen Verbindungen der einzelnen Elemente miteinander

dargestellt sind. Im Beispiel handelt es sich um einen Datenspeicher 102 mit zwei Chipkartenanwendungen A und B, denen je eine Anwendungsbeschreibung ADA 401 und ADB 402 zugeordnet ist. Weiterhin sind der Anwendungsbeschreibung ADA 401 die Personalisierungsbeschreibungen PDA1 403 und PDA2 404, und der Anwendungsbeschreibung ADB 402 die Personalisierungsbeschreibungen PDB1 405 und PDB2 406 zugeordnet. Vorteilhaft ist, wie in Fig.4 dargestellt, daß sowohl Anwendungsbeschreibungen 401, 402 als auch Personalisierungsbeschreibungen 403, 404, 405, 406 in beliebiger Reihenfolge im Datenspeicher 102 der Chipkarte 100 abgelegt sein können.

Nachdem die Initialisierung der Chipkarte 100 beschrieben wurde, wird jetzt näher auf die Personalisierung eingegangen, bei der die geheimen und/oder karten- bzw. nutzerspezifischen Personalisierungsdaten auf die Chipkarte 100 aufgebracht werden. Bei der Beschreibung der einzelnen Schritte der Personalisierung wird auf Fig.6 Bezug genommen. In der beschriebenen Ausführungsform sind die Felder LEN und FLAGS in der Personalisierungsbeschreibung enthalten.

Die Personalisierung erfolgt nun durch das Abarbeiten der PD-Liste für jeden AD 401, 402. Als Beispiel soll hier die Personalisierung einer Chipkartenanwendung A dienen. Dazu wird, wie in Schritt 601 dargestellt, beispielsweise durch einen Operator, welcher die Personalisierung durchführt, ein Personalisierungskommando, beispielsweise in der Form PERSONALIZE (AID, erster Personalisierungsdatensatz), zu der Chipkarte 100 gesendet, das die Kennung AID 301 des der entsprechenden Chipkartenanwendung zugeordneten ADs 401 und einen ersten Personalisierungsdatensatz enthält. Durch die Übermittlung der Kennung AID 301 wird der Personalisierungsvorgang in der Chipkarte 100 angestoßen. Mit Hilfe von Funktionen des Chipkartenbetriebssystems wird der AD der Chipkartenanwendung A, welcher die entsprechenden Kennung

AID aufweist und hier (siehe Fig.4) mit ADA 401 bezeichnet ist, aus den im Datenspeicher 102 vorhandenen ADs 401, 402 ausgewählt, Schritt 602. Für eine fehlerfreie Personalisierung muß der übermittelte Personalisierungsdatensatz diejenigen Daten enthalten, die in das entsprechende erste Personalisierungsdatenfeld, hier PDA1 403, geschrieben werden sollen.

Für den Fall, dass die Chipkarte 100 für eine Nutzung vorgesehen ist, in der lediglich eine einzige Anwendungsbeschreibung AD notwendig ist, kann auf das Vorhandensein der Kennung AID 301 in der Anwendungsbeschreibung und im Personalisierungskommando verzichtet werden.

Anschließend erfolgt in Schritt 603 in der Chipkarte 100 die Überprüfung, ob der Wert im Längenfeld 201 des PD, der über das Offsetfeld ACT 302 des ADA 401 referenziert wird, hier also PDA1 403, identisch ist mit der Länge des im Personalisierungskommando übergebenen Personalisierungsdatensatzes.

Falls dies der Fall ist, wird der Personalisierungsdatensatz in Schritt 604 dahingehend überprüft, ob er den im Statusfeld FLAGS 202 von PDA1 403 definierten Sicherheitsanforderungen genügt. Ist beispielsweise im Statusfeld FLAGS festgelegt, dass die übermittelten Personalisierungsdaten mit einer digitalen Signatur versehen sind, so erfolgt zum Beispiel eine Überprüfung der Personalisierungsdaten dahingehend, ob eine derartige Signatur vorhanden ist und ob diese Signatur unverändert ist. Die Prüfung der Signatur erfolgt zum Beispiel unter Verwendung von Schlüsseldaten KEY 303 aus ADA 401, die einen entsprechenden Signaturschlüssel enthalten können. Ist beispielsweise in dem Statusfeld FLAGS festgelegt, daß die übermittelten Personalisierungsdaten verschlüsselt sind, so

erfolgt zum Beispiel eine Überprüfung dieser Verschlüsselung und/oder eine Entschlüsselung dieser Daten zum Beispiel unter Verwendung von Schlüsseldaten KEY 303 aus ADA 401, die einen entsprechenden kryptographischen Schlüssel enthalten können. Für die Überprüfung von Sicherheitsmerkmalen kann das Personalisierungskommando Vergleichswerte von Prüfsummen etc. enthalten. In Schritt 604 werden bevorzugt alle in Statusfeld FLAGS definierten Sicherheitskriterien abgearbeitet.

Ist diese Sicherheitsprüfung erfolgreich, wird das Offsetfeld ACT 302 in ADA 401 in Schritt 605 mit den in PDA1 403 gespeicherten Offsetfeld NEXT 203 überschrieben. Der (gegebenenfalls entschlüsselte) Personalisierungsdatensatz wird an die Stelle im Datenspeicher 102 geschrieben, an der PDA1 403 gespeichert ist. Da somit PDA1 403 überschrieben wird, wird die Speicherkapazität des Datenspeichers optimal ausgenutzt.

Werden die optionalen Felder nicht verwendet, entfällt die Überprüfung der Länge der Personalisierungsdaten und/oder der Sicherheitsanforderungen, was eine Erhöhung der Personalisierungsgeschwindigkeit zur Folge hat. Im Fall der schnellsten Personalisierung werden die Personalisierungsdaten in ihrer bestimmten Reihenfolge an die Chipkarte 100 übertragen und dort in die dafür vorgesehenen Felder geschrieben. Dabei ist die Trennung der Anwendungen durch das verwendete Adressierungsprinzip durch PD's und AD's gewährleistet.

Bei einer Personalisierung entsprechend der vorliegenden Erfindung ist es nicht erforderlich, neben den eigentlichen Personalisierungsdaten (und der Kennung AID 301 beim Vorhandensein mehrerer Anwendungsbeschreibungen) zusätzliche Informationen über vorhandene Platzhalter an die Chipkarte 100 zu übertragen, da sich alle notwendigen Informationen,

insbesondere über die während der Personalisierung zu verwendenden Speicheradressen, bereits auf der Chipkarte befinden. Entsprechend reduziert sich die für den Personalisierungsvorgang benötigte Datenübertragungszeit. Damit sind wesentlich schnellere Personalisierungen als bisher möglich, insbesondere dann, wenn auf den Einsatz von zeitintensiven Optionen, wie beispielsweise dem Zähler SEQ 305, verzichtet wird.

Die beschriebenen, während des Initialisierungs- und Personalisierungsvorganges notwendigen Vorgänge auf der Chipkarte 100, insbesondere die Schritte 602 bis 607, die durchzuführenden Überprüfungen und Berechnungen, werden auf der Chipkarte 100 mittels entsprechender Programmroutinen, welche zum Beispiel im Chipkartenbetriebssystem implementiert sind, mittels des Prozessors 101 ausgeführt.

Wurde bei der Initialisierung, beispielsweise durch das Setzen eines entsprechenden Bits im Statusfeld FLAGS 202 des PDA1 403, festgelegt, dass der erste Personalisierungsdatensatz mit einer bestimmten Signatur versehen sein muß, so ist aufgrund der Sicherheitsüberprüfung ein Überschreiben von PDA1 403 nur für denjenigen möglich, der einen entsprechenden Personalisierungsdatensatz an die Chipkarte 100 übergibt. Ein versehentliches oder absichtliches Überschreiben von anderen PDs 404, 405, 406 wird dadurch ausgeschlossen. Da für jeden PD 403, 404, 405, 406, also für jedes Personalisierungsdatenfeld, schon bei der Initialisierung eigene Sicherheitsmerkmale definiert werden können, kann die Personalisierung jedes einzelnen Personalisierungsdatenfeldes einzeln gesteuert werden. Dabei können die einmal definierten Sicherheitsmerkmale später nicht mehr umgangen werden.

Alternativ kann während der Initialisierung, beispielsweise durch ein entsprechendes Steuerbit im Statusfeld FLAGS 202,

festgelegt werden, daß der im Personalisierungskommando übergebene Personalisierungsdatensatz kürzer sein darf als vorgesehen, d.h. dass dieser Wert kleiner ist als der Wert im Längenfeld LED 201 des entsprechenden PD. Da in diesem Fall die übertragene Personalisierungsdatenmenge geringer ist, kann der schon reservierte, aber nicht genutzte Speicherplatz im Datenspeicher 102 der Chipkarte 100 mit Füllbytes aufgefüllt werden. Die Sicherheitsprüfung erfolgt also in diesem Fall auch dann, wenn der übertragene Personalisierungsdatensatz kürzer ist als bei der Initialisierung bestimmt.

Die Situation im Datenspeicher 102 der Chipkarte 100 zeigt nun Fig.5, in der wiederum auch die logischen Verbindungen der einzelnen Elemente miteinander dargestellt sind. An der Stelle des PDA1 403 befindet sich der übertragene Personalisierungsdatensatz 500 (in Fig.5 ist der ursprüngliche Platz von PDA1 403 mit gestrichelten Linien angedeutet). Das Offsetfeld ACT 302 von ADA 401 zeigt auf PDA2 404. Die Datenstrukturen (ADB, PDB1, PDB2) für die Chipkartenanwendung B sind unverändert.

Im nächsten Personalisierungskommando kann, beispielsweise mit einem Personalisierungskommando der Form PERSONALIZE (AID, zweiter Personalisierungsdatensatz), PDA2 404 überschrieben werden. Alternativ könnte mit dem Überschreiben von PDB1 405 begonnen werden, usw. Zu beachten ist, dass die Reihenfolge der zu übertragenden Personalisierungsdatensätze 500 der Verbindung der PDs 403, 404, 405, 406 in den jeweiligen PD-Listen entsprechen muß. Hierbei kann unterstützend zum Beispiel der Zähler SEQ 305 verwendet werden.

Sind alle PDs eines AD überschrieben, d.h. enthält die PD-Liste keine weiteren Elemente, was dadurch gekennzeichnet sein kann, dass das Offsetfeld NEXT 203 des letzten PD den

Inhalt Null hat, so wird in Schritt 607 der verwendete AD der entsprechenden Chipkartenanwendung gelöscht. Die Chipkartenanwendung ist komplett geladen.

In einer Ausführungsform der Erfindung wird die Kennung AID 301 in dem Personalisierungskommando lediglich in den Fällen übertragen, in denen eine neue Anwendungsbeschreibung AD ausgewählt werden soll, beispielsweise bei der Übertragung des ersten Personalisierungskommandos. Solange eine darauffolgendes Personalisierungskommando keine Kennung AID 301 enthält, erfolgt die Zuordnung der übertragenen Personalisierungsdaten zu der entsprechenden Anwendungsbeschreibung automatisch, beispielsweise unter Verwendung entsprechender Funktionen des Chipkartenbetriebssystems. Erst bei der Übertragung einer weiteren Kennung AID 301 wird erneut ein entsprechender AD ausgewählt.

Die Personalisierung auf der Chipkarte 100 erfolgt unter Verwendung bekannter, zum Beispiel zuvor definierter Dienste und Routinen des Chipkartenbetriebssystems, die durch Kommandos, beispielsweise durch die Personalisierungskommandos, aufgerufen werden können.

P A T E N T A N S P R Ü C H E

1. Verfahren zum Initialisieren und Personalisieren einer Chipkarte (100), wobei Daten für mindestens eine Chipkartenanwendung in den Datenspeicher (102) der Chipkarte (100) übertragen werden, mit den Schritten

während der Initialisierung:

- Schreiben mindestens einer Anwendungsbeschreibung (300) für eine Chipkartenanwendung in den Datenspeicher (102) der Chipkarte (100), wobei die Anwendungsbeschreibung (300) Angaben (302) über eine Speicheradresse genau einer Personalisierungsbeschreibung (200) umfaßt,
- Schreiben mindestens einer Personalisierungsbeschreibung (200) in den Datenspeicher (102) der Chipkarte (100), wobei die Personalisierungsbeschreibung (200) Angaben (203) über eine Speicheradresse einer nächsten Personalisierungsbeschreibung (210) umfaßt, und

während der Personalisierung:

- Übertragen der Personalisierungsdaten (500) für eine Chipkartenanwendung an die Chipkarte (100),
- Schreiben der Personalisierungsdaten (500) in den Datenspeicher (102) der Chipkarte (100) an die Speicheradresse entsprechend den Angaben (302) in der Anwendungsbeschreibung (300),
- Übergeben der Angaben (203) über die Speicheradresse der nächsten Personalisierungsbeschreibung (210) aus der Personalisierungsbeschreibung (200) an die Anwendungsbeschreibung (300), derart, daß der

Anwendungsbeschreibung (300) dann die nächste Personalisierungsbeschreibung (210) zugeordnet ist,

- Wiederholen der Personalisierungsschritte für alle zu übertragenden Personalisierungsdaten.

2. Verfahren nach Anspruch 1, wobei die Anwendungsbeschreibung (300) Angaben (301) für eine eindeutige Zuordnung der Anwendungsbeschreibung (300) zu einer Chipkartenanwendung umfaßt.

3. Verfahren nach Anspruch 1 oder 2, wobei die Personalisierungsbeschreibung (200) zusätzlich Angaben (201, 202) umfaßt, welche die Eigenschaften der zu übertragenden Personalisierungs-daten (500) beschreiben, und mit dem zusätzlichen Schritt:

- Überprüfen der übertragenen Personalisierungsdaten (500) dahingehend, ob sie die Angaben (201, 202) erfüllen;

und wobei das Schreiben der Personalisierungsdaten (500) in den Datenspeicher (102) der Chipkarte (100) nur dann erfolgt, wenn die Angaben (201, 202) erfüllt sind.

4. Verfahren nach Anspruch 3, wobei die Personalisierungsdaten (500) hinsichtlich der Angaben (201, 202) aus derjenigen Personalisierungs-beschreibung (200) überprüft werden, die der Anwendungsbeschreibung (300) aktuell zugeordnet ist.

5. Verfahren nach Anspruch 3 oder 4, wobei die Personalisierungsdaten (500) unter Verwendung von Informationen (303) überprüft werden, die in der Anwendungsbeschreibung (300) enthalten sind.

6. Verfahren nach einem der Ansprüche 3 bis 5, wobei die in der Personalisierungsbeschreibung (200, 210) enthaltenen Angaben (201, 202) die Länge (201) der Personalisierungsdaten (500) umfassen.

7. Verfahren nach einem der Ansprüche 3 bis 6, wobei die in der Personalisierungsbeschreibung (200, 210) enthaltenen Angaben (201, 202) Sicherheitsanforderungen (202), die an die Personalisierungsdaten (500) gestellt werden, umfassen.

8. Verfahren nach einem der Ansprüche 1 bis 7, wobei die Anwendungsbeschreibung (300) einen Zähler (305) umfaßt, und mit dem zusätzlichen Schritt

- Inkrementieren des Zählers (305) bei jedem erfolgreichen Eintragen eines Personalisierungsdatensatzes in den Datenspeicher (102) der Chipkarte (100).

9. Chipkarte (100) mit Prozessor (101) zum Ausführen von Programmroutinen, Datenspeicher (102) und Programmroutinen zum Ausführen des Verfahrens nach einem der Ansprüche 1 bis 8.

10. Chipkarte nach Anspruch 9, wobei der Datenspeicher (102) vor Beginn der Personalisierung der Chipkarte (100) umfaßt:

mindestens eine Anwendungsbeschreibung (300) einer Chipkartenanwendung, die Angaben (302) über eine Speicheradresse einer Personalisierungsbeschreibung (200) umfaßt, sowie

mindestens eine Personalisierungsbeschreibung (200), die Angaben (203) über eine Speicheradresse einer nächsten Personalisierungbeschreibung (210) umfaßt.

11. Chipkarte nach Anspruch 10, wobei die Anwendungsbeschreibung (300) Angaben (301) über die ihr zugeordnete Chipkartenanwendung umfaßt.

12. Chipkarte nach Anspruch 10 oder 11, wobei die Anwendungsbeschreibung (300) Informationen (303) umfaßt, die zu einer Überprüfung der Personalisierungsdaten (500) verwendet werden können.

13. Chipkarte nach Anspruch 10 bis 12, wobei die Personalisierungsbeschreibung (200) zusätzliche Angaben (201, 202) umfaßt, welche die Eigenschaften der zu übertragenden Personalisierungsdaten (500) beschreiben.

14. Verfahren nach einem der Ansprüche 10 bis 13, wobei die Anwendungsbeschreibung (300) einen Zähler (305) umfaßt, der bei jedem erfolgreichen Eintragen eines Personalisierungsdatensatzes in den Datenspeicher (102) der Chipkarte (100) inkrementiert wird.

Z U S A M M E N F A S S U N G

Die Erfindung betrifft ein Verfahren zum Initialisieren und Personalisieren einer Chipkarte (100) und eine entsprechende Chipkarte (100). Entsprechend der vorliegenden Erfindung werden im Datenspeicher (102) der Chipkarte (100) Datenstrukturen (200, 210, 300) angelegt, die eine eindeutige Zuordnung der bei der Personalisierung auf die Chipkarte (100) zu übertragenden Personalisierungsdaten zu den einzelnen Chipkartenanwendungen und damit zu den Anbietern dieser Chipkartenanwendungen ermöglicht. Dadurch wird eine sichere Trennung der Chipkartenanwendungen bei der Personalisierung realisiert.

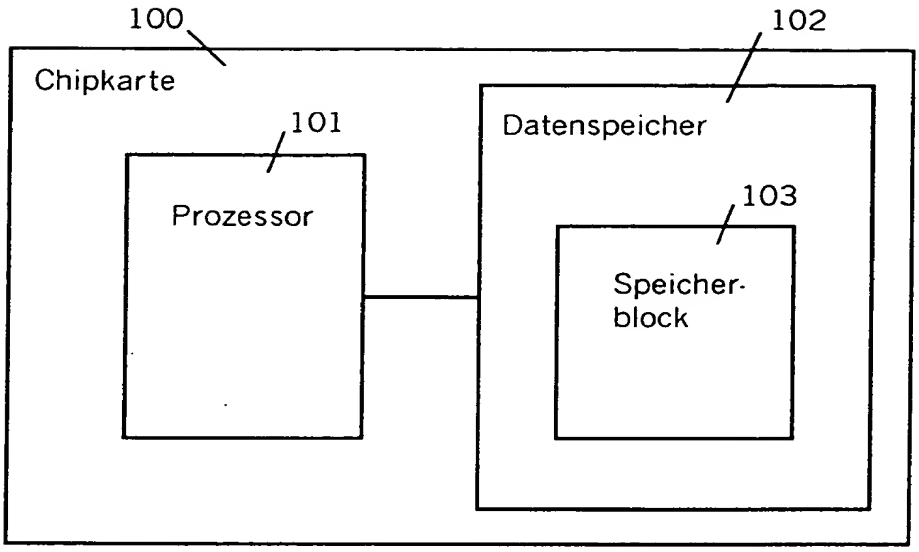
100
Chipkarte
101
Prozessor
102
Datenspeicher
103
Speicher-
block

FIG.1

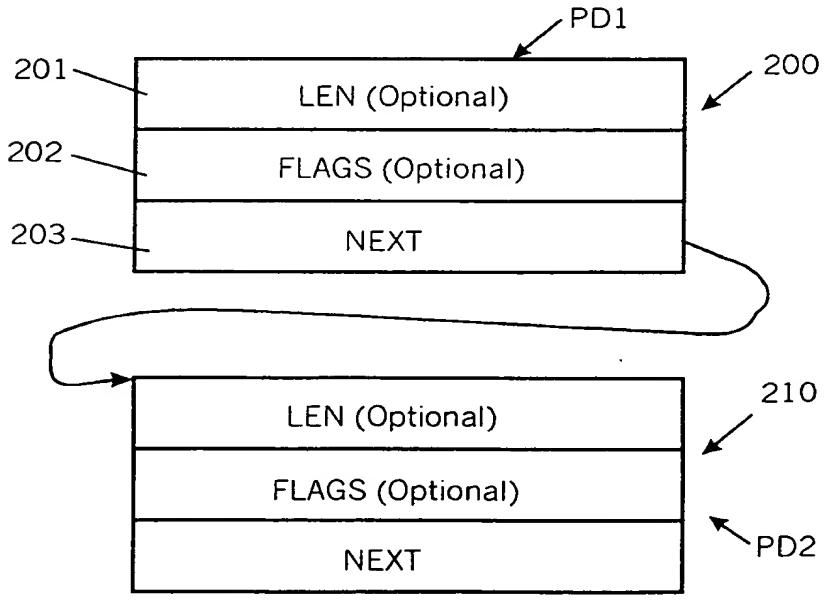
PD1
201
200
LEN (Optional)
202
FLAGS (Optional)
203
NEXT
LEN (Optional)
210
FLAGS (Optional)
NEXT
PD2

FIG.2

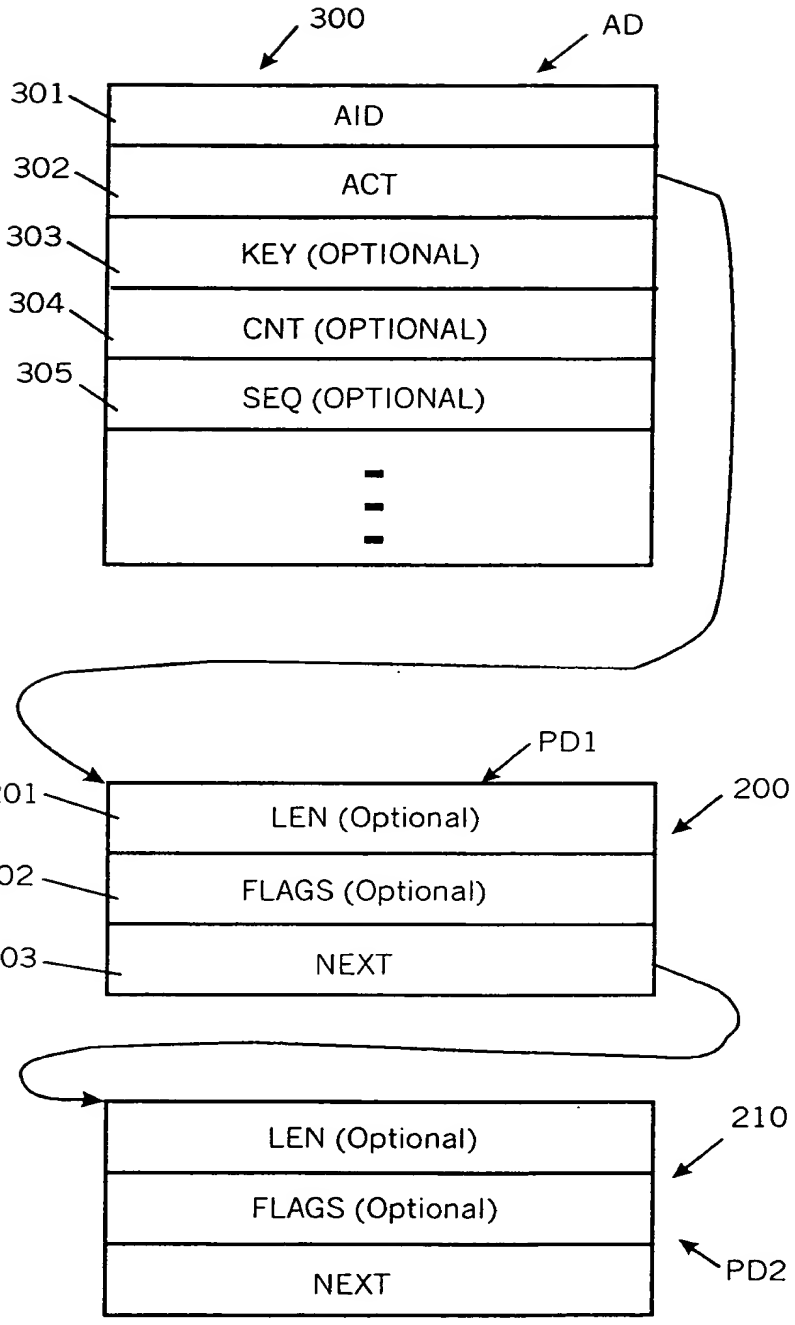
300
AD
301
AID
302
ACT
303
KEY (OPTIONAL)
304
CNT (OPTIONAL)
305
SEQ (OPTIONAL)
PD1
201
LEN (Optional)
200
202
FLAGS (Optional)
203
NEXT
LEN (Optional)
210
FLAGS (Optional)
NEXT
PD2

FIG.3

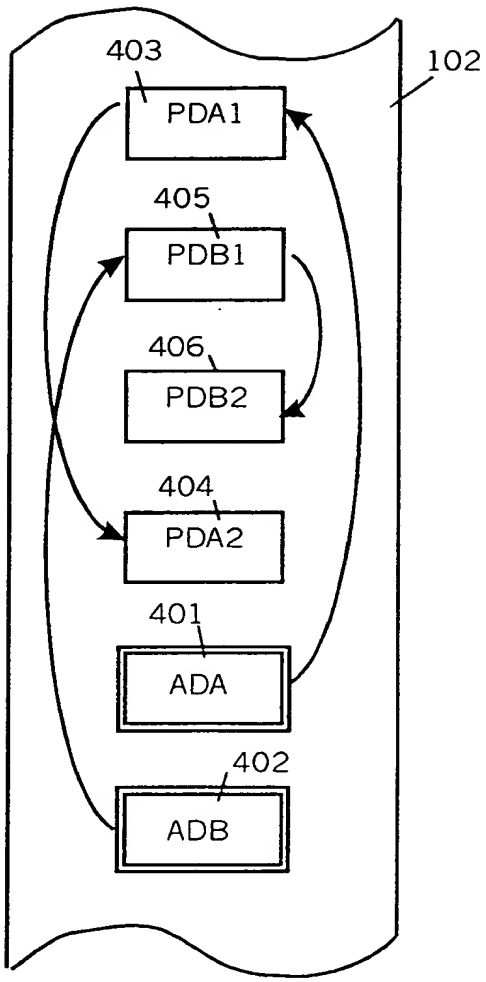
403
102
PDA1
405
PDB1
406
PDB2
404
PDA2
401
ADA
402
ADB

FIG.4

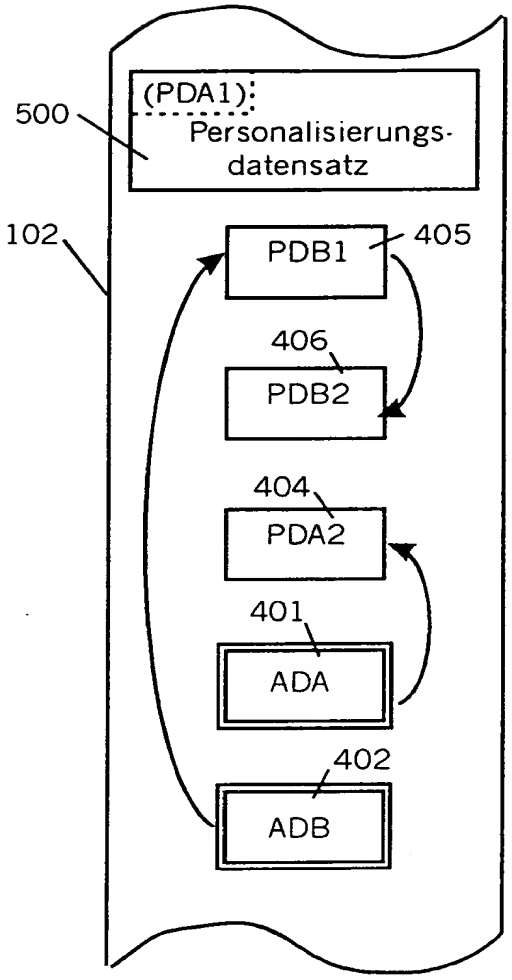
(PDA1):
Personalisierungs-
datensatz
500
102
PDB1
405
406
PDB2
404
PDA2
401
ADA
402
ADB

FIG.5

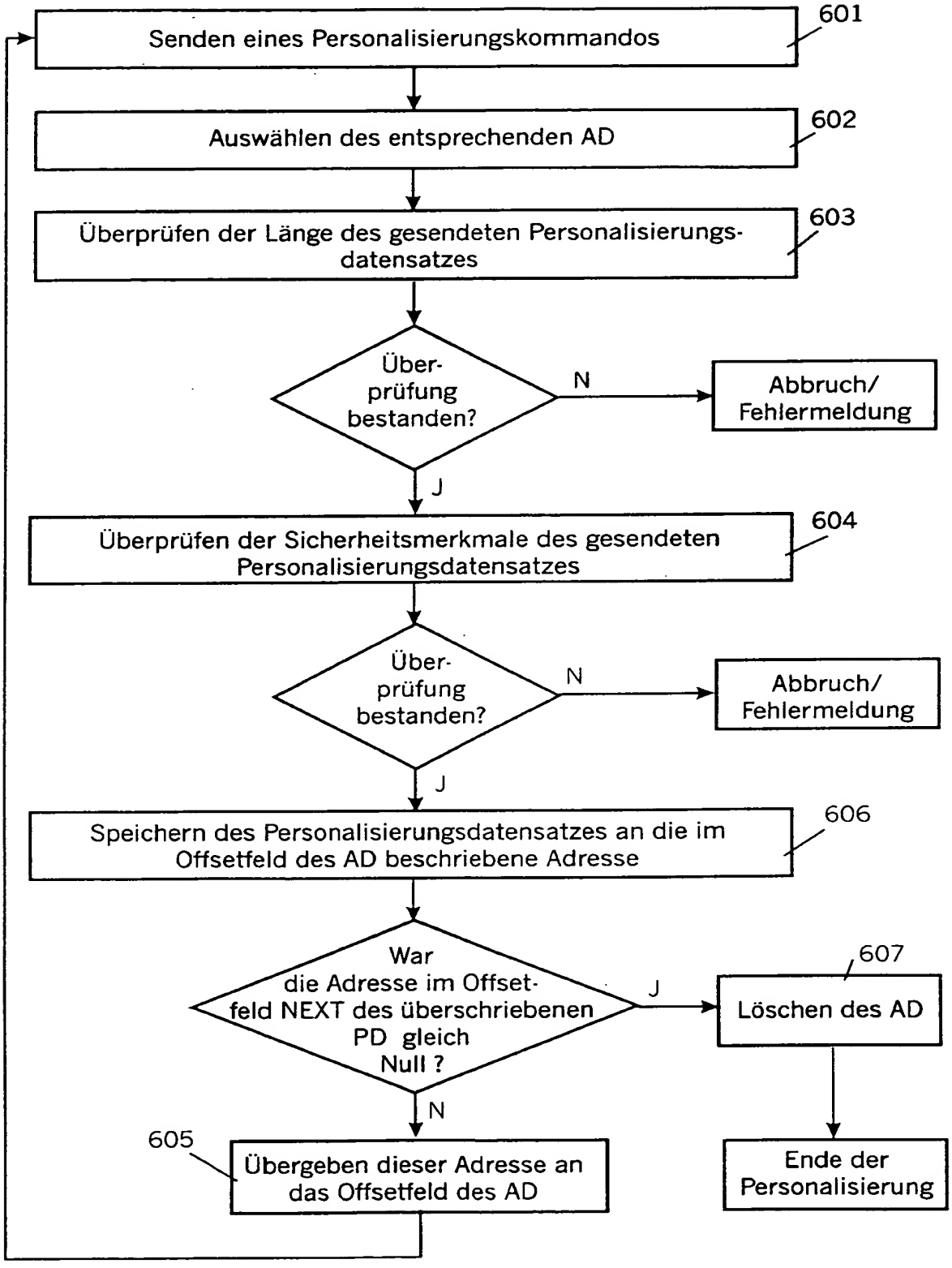
Senden eines Personalisierungskommandos
601
Auswählen des entsprechenden AD
602
Überprüfen der Länge des gesendeten Personalisierungs-datensatzes
603
Über-prüfung bestanden?
N
Abbruch/ Fehlermeldung
J
Überprüfen der Sicherheitsmerkmale des gesendeten Personalisierungsdatensatzes
604
Über-prüfung bestanden?
N
Abbruch/ Fehlermeldung
J
Speichern des Personalisierungsdatensatzes an die im Offsetfeld des AD beschriebene Adresse
606
War die Adresse im Offset-feld NEXT des überschriebenen PD gleich Null ?
J
607
Löschen des AD
N
605
Übergeben dieser Adresse an das Offsetfeld des AD
Ende der Personalisierung

FIG.6